Jaarverslag Toezicht Informatiebeveiliging en Privacy 2022

Chief Information Security Officer en

Functionaris gegevensbescherming

Inleiding

Een gemeente verwerkt op grote schaal informatie en persoonsgegevens van inwoners, andere betrokken relaties en eigen medewerkers. De Baseline Informatiebeveiliging Overheid (BIO), Europese Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) bieden waarborgen voor het beschermen van deze gegevens. Zij verplichten tot het aantoonbaar treffen van maatregelen om informatieveiligheid en privacy te borgen. In dit jaarverslag brengen de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) als onafhankelijk toezichthouders verslag uit over de naleving van de BIO en de AVG bij gegevensverwerkingen die onder de verantwoordelijkheid van het college en de gemeenteraad worden uitgevoerd. De CISO en de FG adviseren daarbij over de te nemen maatregelen.

De top vijf aanbevelingen van het de CISO en FG:

1. Stel nieuw beleid vast voor informatiebeveiliging en privacy
2. Richt het procesmanagement in en stel hier governance voor op
3. Creëer overzicht met de verplichte documenten en processen
4. Reageer op de aanbevelingen uit de toezichtsonderwerpen 2022
5. Implementeer de WPG-verplichte documenten en processen

In dit jaarverslag leest u het verslag van de CISO en de FG over 2022 met de aanbevelingen die de organisatie in 2023-2024 gaat uitvoeren.

Inhoud:

Inhoud

Terugblik 2022

Eind 2021 heeft een extern bureau M&I een onderzoek[1] gedaan naar de privacyvolwassenheid van de gemeente Westerveld. Deze zijn voorjaar 2022 besproken binnen de organisatie. Dit zijn hun aandachtspunten:

1. Beleid
   Het huidige verouderde privacybeleid moet worden herijkt
2. Governance en processen
   a. Eigenaarschap
      de lijn, de leidinggevenden zijn de proceseigenaren en als zodanig verantwoordelijk voor het voldoen aan privacy- en informatiebeveiligingsvereisten
   b. Formatie van het privacyteam
      uitbreiding Privacy Officer formatie naar 32 / 36 uur[2]
   c. Bewustwording over privacy en informatiebeveiliging
      als een taak van de leidinggevenden
3. Overzicht
   a. Het Register van Verwerkingen
      up to date met dataclassificatie; beheer en actualisatie belegd
   b. Risicomanagement:
      afwegingen over privacy en informatiebeveiliging vooraan in het (inkoop)proces en vastleggen in een risicoregister
   c. Autorisatiemanagement
      leg functies en rollen vast en let op bij wijzigingen
   d. Informatie op Webveld
      indikken en actualiseren

1. Beleid

Uit het onderzoeksrapport van M&I is gebleken dat bij het management en het bestuur (te) weinig aandacht is voor en kennis over het beschermen van persoonsgegevens en informatiebeveiliging. Er is niets over vermeld bij de collegevorming en is er geen portefeuillehouder specifiek aangewezen. Het huidige Privacybeleid van 2018 is verouderd, want nieuwe ontwikkelingen zijn niet meegenomen en de gemeentelijke organisatie is sindsdien veranderd.

Advies 1: Gelet op de samenhang tussen privacy en informatiebeveiliging, wordt door de FG en CISO een samenhangend beleid tussen beide aangeraden.

Reactie MT: Conform. In 2023-2024 wordt hiervoor budget gevraagd.

2. Procesmanagement en governance

a. Eigenaarschap 'three lines of defence'

Het privacyteam bestaat uit een Privacy Officer, CISO en FG. De Privacy Officer adviseert en ondersteunt de gemeentelijke organisatie over de naleving van de privacywetgeving en is het eerste aanspreekpunt voor privacyvragen. De FG is verantwoordelijk voor het toezicht op de naleving van

[1] Bijlage 1: Uittreksel van het rapport van M&I
[2] was toen 18, is nu 28 uur

de privacywetgeving en is onafhankelijk adviseur voor management en bestuur. De CISO is verantwoordelijk voor het toezicht op de naleving van de informatiebeveiliging, de BIO en rapporteert hierover middels de ENSIA (eenduidige normatief single information audit)[3].De taken van het privacyteam zitten in de tweede en derde lijn[4].

De teamleiders zijn als eerste lijn integraal proceseigenaar en verantwoordelijk voor alle teamprocessen en dus voor het beleid, de uitvoering, de monitoring én de bedrijfsvoeringstaken. Daar horen ook gegevensbescherming en informatiebeveiliging bij. Deze rolverdeling is nog niet voor iedereen duidelijk.

Advies 2: De FG en CISO raden aan eigenaarschap en three lines of defence vast te leggen in een governance voor privacy- en informatiebeveiliging[5].

Reactie MT: Conform.

b. Formatie van het privacyteam

Vanaf mei 2022 is de formatie voor de Privacy Officer uitgebreid naar 28 uur. M&I heeft geconcludeerd dat 32 tot 36 uur nodig zou zijn. Terugkijkend op 2022 wordt duidelijk dat de inschatting van M&I juist lijkt, want het is in 2022 niet gelukt om de aanbevelingen van M&I op te pakken. Er zijn teveel “dagelijkse vragen” en ontwikkelingen die vanuit privacy en informatiebeveiliging aandacht vragen. Ook is er is veel verloop in de organisatie. Daarnaast is de Privacy Officer belast met de Wpg-audit en het coördineren van het Wpg-verbeterplan. Hierdoor loopt de achterstand in het op orde brengen van de verplichte processen en procedures verder op. Vanaf medio 2018 hadden de gemeenten Staphorst, Steenwijkerland, Westerveld en Zwartewaterland een samenwerking voor twee FG’s; in elke gemeente 18 uur. In september 2022 is de samenwerking met de gemeenten Staphorst en Zwartewaterland beëindigd. De FG-formatie is nu 14 uur. M&I raamde de benodigde FG-inzet op 18 uur.

Advies 3: De FG en de CISO raden aan om in 2023 en 2024 de prioriteit te leggen op de verplichte AVG, BIO en Wpg-producten, ook al gaat dit ten koste van de inzet van het privacyteam op actuele vragen en ontwikkelingen. Dit betekent voor 2023 en 2024 meer risico’s op datalekken, incidenten, risicovolle inrichtingen en risicovol beheer van processen. Dit is echter nodig om binnen de huidige formatie een structurele verbetering in de AVG en BIO-compliancy te kunnen realiseren. Dit zal overigens ook inzet uit de rest van de organisatie vragen.

Reactie MT: Conform. Hiermee neemt de gemeente een risico met als doel om binnen de bestaande formatie de vereiste structurele processen en producten in twee jaar tijd op orde te krijgen.

C. Bewustwording

Binnen alle geledingen van de organisatie is de kennis over privacy en informatiebeveiliging laag. Alle nieuwe medewerkers worden nu uitgenodigd om binnen drie maanden de e-learning privacy en informatiebeveiliging van de VNG te volgen. Eind 2022 is de gemeente Westerveld gestart met een online leerplatform; Leerveld. Hierin staan ook trainingen over AVG en BIO, zoals Privacy Awareness, Security Awareness en datalekken. In 2022 bestond nog geen relatie tussen het wel of niet afronden

[3] Op 18 april 2023 heeft de CISO de ENSIA-rapportage voorgelegd aan het college. Dit rapport staat hier los van.
[4] Zie ook: Three lines model - Accent Advies
[5] Governance = de sturing, verantwoording en monitoring van beleid, procedures en maatregelen om de organisatie te kunnen laten functioneren in overeenstemming met haar doelstellingen.

van de training en het toewijzen van autorisaties. Daardoor was nog niet geborgd dat nieuwe medewerkers veilig met (persoons-)gegevens (kunnen) omgaan.

Advies 4: De CISO en FG adviseren om een bewustwordingsprogramma op te zetten en om voor hoog-risicovolle applicaties verplichte trainingen te eisen voordat hiermee gewerkt mag worden.

Reactie MT: Conform. In 2023-2024 wordt budget gevraagd om een bewustwordingsprogamma op te zetten en uit te voeren.

3. Overzicht

a. Register van verwerkingen en dataclassificatie

Gemeenten moeten kunnen aantonen dat zij handelen in overeenstemming met de AVG. Dat betekent dat zij onder andere een register van verwerkingsactiviteiten dienen bij te houden. Het doel van dit register is inzicht in de structurele verwerkingen en daarbij gebruikte persoonsgegevens binnen de organisatie en overzicht op de meest risicovolle processen. Door toepassing van dataclassificatie is duidelijk welke verwerkingen het meest risicovol zijn. Het register van de gemeente Westerveld is onvolledig en niet actueel. Daardoor is onbekend welke verwerkingen met persoonsgegevens er binnen de gemeente zijn en welke risico's de gemeente hiermee loopt. Privacy en informatiebeveiligingsrisico's zijn daardoor onvoldoende in beeld.

Advies 5: De CISO en FG adviseren om verplichte formats voor het Register van verwerkingen en dataclassificatie op te stellen en daarna bij de teams toe te lichten voor beheer en gebruik ervan.
Reactie MT: Conform.

Dataclassificatie

Het belang van informatie classificeren is inzicht krijgen in de waarde van informatie op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Deze zijn onder andere van belang voor bedrijfscontinuïteit (beschikbaarheid) en de juistheid en zorgvuldigheid van de gegevens (integriteit). Vanuit privacy is het aspect vertrouwelijkheid het grootst. Bij een BIV classificatie wordt de waarde van informatie bepaald. Aan de hand daarvan worden passende maatregelen genomen om deze gegevens te beschermen. De BIO vereist dat in projecten beveiligingsrisico's en maatregelbepaling zijn opgenomen als onderdeel van het ontwerp.

Advies 6: De CISO en FG adviseren te bepalen wat hoog-risicovolle applicaties zijn en per applicatie een autorisatiematrix op te stellen en vast te laten stellen.
Reactie MT: Conform.

b. *Risicomanagement, privacy -en informatiebeveiligingsrisico's in beeld*

Op grond van de AVG zijn gemeenten verplicht om data protection impact assessments (DPIA's[6]) uit te voeren voor verwerkingen van persoonsgegevens met een hoog risico. Daarvan is bijvoorbeeld sprake wanneer de gemeente bijzondere persoonsgegevens[7] zou gaan verwerken of gaat delen met

[6] Een DPIA is een analysetool om de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen of kan besluiten de (rest)risico's te aanvaarden.
[7] Zie art. 9 AVG en art. 5 Wpg, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#bijzondere-persoonsgegevens

een andere gemeente of instantie. Met een DPIA wordt voorafgaand aan een hoog-risicovolle verwerking een beoordeling uitgevoerd van de effecten van de beoogde activiteiten op de bescherming van persoonsgegevens. Ook van bestaande risicovolle verwerkingen moet in kaart worden gebracht welke maatregelen de privacy- en informatiebeveiligingsrisico's ondervangen en wat het eventuele restrisico is. Na het doorlopen van de DPIA geeft de FG advies en besluit de organisatie om de voorgestelde maatregelen te nemen en/of om eventuele restrisico's te accepteren.

Begin 2022 is door het privacyteam van de gemeente Westerveld namens de zeven Zuid-Drentse gemeenten een DPIA gedaan op het Dashboard Jeugdhulp Zuid-Drenthe. Hierin worden o.a. medische gegevens verwerkt van degenen die jeugdzorg ontvangen van een van deze zeven gemeenten. Met dit dashboard hebben de gemeenten een prognosetool per aanbieder en gemeente dit kan als benchmark worden gebruikt. De voorgestelde en afgesproken mitigerende maatregelen zijn gericht op het anoniem verwerken van de gegevens en het maken van duidelijke verwerkersafspraken mejkt de uitvoerende instantie.

In 2022 zijn in Westerveld verder geen DPIA's gedaan. Dat is onder de maat: er zijn in elke gemeente elk jaar nieuwe en bestaande hoog-risicovolle verwerkingen. Zo starten er regelmatig nieuwe processen en applicaties die gevolgen hebben voor de toegang tot risicovolle persoonsgegevens (bijvoorbeeld het nieuwe Zaaksysteem).

Advies 7: De FG en CISO adviseren de organisatie om DPIA's uit te voeren voor gegevensverwerkingen met een hoog risico en vraagt de organisatie om voor onderwerpen waarvoor in 2023 en 2024 DPIA's moeten worden gemaakt een DPIA-kalender te maken.

Reactie MT: Conform.

c. *Autorisatiemanagement*

De Ondernemingsraad heeft gevraagd om de medewerkers duidelijkheid te geven over de autorisaties en wat ze wel en niet mogen. De AVG vereist dat autorisaties goed zijn ingericht vanuit de principes least-privileged en need to know: dat is dat zo min mogelijk - alleen diegene voor wiens werk dat echt nodig is - medewerkers de persoonsgegevens kunnen inzien en bewerken. De BIO verreist dat de gemeente een vastgesteld screeningsbeleid heeft en dat bij indiensttreding en bij functiewijziging een verklaring omtrent gedrag (VOG) gevraagd wordt. Hieraan voldoet de gemeente Westerveld nog niet.

Advies 8: De FG en CISO raden het MT aan om het proces voor autorisaties en VOG aan te scherpen door te checken op de verplichte trainingen, de VOG en de autorisaties bij het 100 dagen-gesprek met de nieuwe medewerker.
Reactie MT: Conform.

d. *Informatie op Webveld (intranet)*

De medewerkers moeten op één plek alle informatie over privacy en informatiebeveiliging kunnen vinden. Dat wat nu op Webveld staat, kan beter en duidelijker.

Advies 9: De FG en CISO adviseren om de informatie op Webveld te vernieuwen wanneer de formats en nieuwe documenten voor alle verplichte producten en processen gereed zijn.
Reactie MT: Conform.

4. Toezichtkalender FG en CISO 2022

In de FG-en CISO-jaarkalender 2022[8] staan de volgende onderzoeken voor 2022:
Q1: Bevragingen aan het Inlichtingenbureau door de gemeente. De Autoriteit Persoonsgegevens (AP) heeft in een brief aan de VNG kenbaar gemaakt de indruk te hebben dat gemeenten mogelijk teveel en te frequent persoonsgerelateerde informatie over (uitkeringsgerechtigde) inwoners uitvragen. De AP gaat hier streng op toezien.
Q2: Processen jeugd, met name informatieplicht naar betrokkenen en transparantie
Q3: Bewustzijn medewerkers m.b.t. datalekken
Q4: Privacy- volwassenheid organisatiebreed en AVG processen
Voor onderzoeken Q3 en Q4 was helaas in 2022 onvoldoende capaciteit en informatie beschikbaar en deze zijn niet uitgevoerd. De inrichting van een privacymanagementtool waarin de informatie over de privacyvolwassenheid en de AVG-verplichte processen overzichtelijk worden weergegeven is nog niet gerealiseerd.

Advies 10:
De FG en CISO adviseren om te onderzoeken hoe en welke privacymanagementtool gebruikt kan worden nadat de bovengenoemde verplichte AVG-processen en producten zijn gerealiseerd.
Reactie MT: Conform.

Q1 Bevragingen Inlichtingenbureau
De FG heeft geoordeeld dat niet is vast te stellen dat de gemeente Westerveld voldoende maatregelen heeft getroffen om bij de bevragingen aan het Inlichtingenbureau te kunnen voldoen aan de AVG. Er is niet vastgesteld dat de gemeente geen grotere inbreuk maakt op de persoonlijke levenssfeer van uitkeringsgerechtigden dan noodzakelijk is.

Advies 11:
De FG adviseert om de belangrijkste aanbevelingen uit te voeren dan wel hierop te reageren.
Reactie MT: Conform.

Q2 Transparantie in jeugdprocessen
De CISO constateert dat binnen de jeugdprocessen opzet en werking van passende technische en organisatorische maatregelen voor de toegang tot systemen grotendeels aanwezig zijn. Wat nog ontbreekt zijn autorisatiematrices voor ieder systeem dat in gebruik is op basis van rollen. De toegang moet aldus worden ingericht, beheerd en (steekproefsgewijs) gecontroleerd.

De FG oordeelt dat binnen de jeugdprocessen nog onvoldoende opzet aanwezig is om te kunnen voldoen AVG-beginselen van informatieplicht en transparantie. Er is bij de jeugdconsulenten zeker aandacht voor de privacy-rechten van betrokkenen en het hierbij betrekken van betrokkenen, maar dit is (nog) niet vastgelegd in een (beschreven) werkproces of werkinstructie en het ontbreekt nog om betrokkenen te informeren over diens AVG-rechten.

Advies 12:
De FG adviseert om de belangrijkste aanbevelingen uit te voeren dan wel hierop te reageren.
Reactie MT: Conform.

[8] B&W 1 maart 2022, AT 10 februari 2022

5. De Wet politiegegevens

Per 1 januari 2019 is de Wet Politiegegevens (Wpg) in werking getreden. In de Wpg is voor werkgevers van BOA's de verplichting opgenomen om elk jaar een interne audit te doen en één keer in de vier jaar een externe audit en de resultaten van de externe audit te delen met de Autoriteit Persoonsgegevens (AP). In 2022 heeft de gemeente Westerveld de externe Wpg-audit laten doen en daarop wordt nu door de organisatie een verbeterplan gemaakt.

Voor de Wpg moet ook een FG worden aangesteld. In Westerveld is nog geen specifieke Wpg-FG aangewezen. De Wpg-FG moet elk jaar een verslag met bevindingen opstellen over de naleving van de Wpg en heeft een adviesrol bij de Wpg-DPIA's. Volgens de NOREA-handreiking (norm 31) moet de Wpg-FG toezicht houden op:

- Het naleven van de Wpg
- Het beleid van de gemeente met betrekking tot de bescherming van persoonsgegevens
- De toewijzing van de autorisaties
- De bewustmaking en opleiding van de boa's en andere functionarissen die betrokken zijn bij de verwerking van persoonsgegevens
- De audit.
- De uitvoering van de DPIA's. In 2023 zijn dat (in ieder geval) DPIA's Boa domeinen I en III.

Advies 13: De FG en CISO adviseren om de Wpg-taken binnen de organisatie te beleggen, voor toezicht op de Wpg een FG aan te wijzen en om een interne/externe auditor te benoemen.

Reactie MT: Conform

6. Behandelen klacht en vraag inwoner

De AVG verplicht gemeenten om de contactgegevens van de FG te publiceren zodat betrokkenen contact kunnen opnemen met deze functionaris. In 2022 hebben twee personen van deze mogelijkheid gebruik gemaakt. De binnengekomen vragen en klachten over de AVG zijn door de FG onderzocht en afgehandeld.

De eerste klacht behelsde dat voor het bijhouden van het Nachtverblijfregister alle namen, adressen en geboortedata van de gasten bijgehouden moeten worden. Hierop is door de gemeenteraad de Toeristenverordening gewijzigd. De klager is daarover geïnformeerd.

Een andere klacht betrof een datalek waardoor het (geheime) adres van de klager herleidbaar werd. De organisatie heeft maatregelen getroffen om de zichtbaarheid van het adres te verminderen en met het team is het werkproces doorgenomen en herzien. De klager claimt verder schadevergoeding. Dit verzoek is afgedaan.

7. Rechten van betrokkenen

De burger heeft op basis van de AVG verschillende rechten om controle te houden over diens persoonsgegevens. Dit worden de rechten van betrokkenen genoemd. De gemeente moet deze verzoeken als verwerkingsverantwoordelijke afhandelen. De procedure wordt in Westerveld gecoördineerd door de privacy officer. Er zijn ongeveer vier inzageverzoeken ontvangen, maar heel duidelijk weten we het niet: er is soms nog onduidelijkheid of een inzageverzoek een AVG- , WMO- of Jeugdwet-inzageverzoek is.

Het proces om binnen de gemeente de gevraagde persoonsgegevens in te zien, wordt door de privacy officer in 2023 vernieuwd.

Advies 14: De FG en CISO adviseren om het proces inzageverzoeken door te ontwikkelen.

Reactie MT: Conform.

8. Incidenten en datalekken

Aantal 2022: 21 incidenten gemeld, waarvan 11 datalekken; drie gemeld aan Autoriteit Persoonsgegevens, 10 gemeld aan betrokkenen. De meeste komen door verkeerde adressering per post of mail. Dit kan vervelend zijn voor de betrokkenen, zeker als het gaat om gevoelige informatie of kwetsbare personen. Daarom is het belangrijk dat medewerkers ook in 2023 gewezen worden op de risico's bij het versturen van persoonsgegevens en gerichte trainingen volgen.

Incidenttype /Oorzaak	**Oorzaken en maatregelen o.a.**
Onveilig menselijk handelen 11x	1x Adresinformatie en 1x een document van een betrokkene op gemeentelijke website: daarvan afgehaald en zoekmachines gevraagd deze te verwijderen. Proces besproken met betrokken team en aangepast. 1x Per ongeluk binnen de organisatie een bestand verstuurd met namen en inschaling van de eigen medewerkers 8x Verkeerde e-mail en onbedoelde ontvangers per email gevraagd deze te verwijderen. Hiervan 1x emailadres met typefout, 1x emailadres (intern) aangepast , 1x verzendlijst gecontroleerd en herzien; 1x aanvrager had zelf verkeerd emailadres ingevoerd en 1x mailadressen niet in bcc gezet
Kwetsbaar-heid in systeem 8x	2x Automatische suggestie adresregel in email 1x Melding door medewerker van verdachte mail met bijlages 2x Technische fouten en 1x wijziging in een systeem 1x Kwetsbaarheden doorgegeven aan leverancier en beheerder ONS 1x Informeren over openbaar maken in Zaaksysteem 1x Procedure voor werkplekbeheer niet gevolgd
Verkeerd of onrechtmatig gebruik van resources 1x	Door onjuiste classificatie zijn in de Basisregistratie Adressen en Gebouwen adressen verwijderd. Dit is hersteld

Programma technische fout 1x	Onvoldoende interne controle en met leverancier besproken
Programma-fouten 2x	Verkeerd geadresseerde brieven: proces uitgaande post herzien
Ongeautorise erde modific-catie / wijziging 1x	Verdwenen / niet opgeslagen documenten in Zaaksysteem. Actie bij leverancier gevraagd

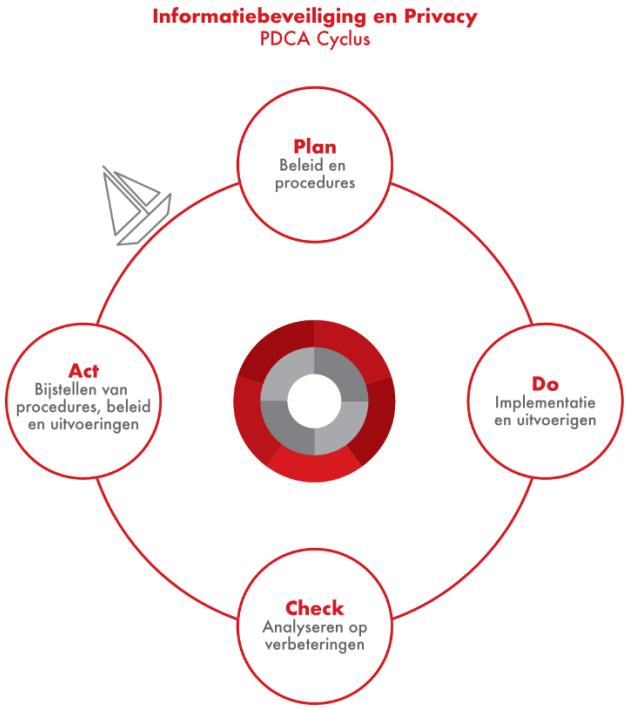
PDCA-cyclus bij datalekken/incidenten:

- Plan: Medewerker meldt een incident/datalek; teamleider wordt geïnformeerd; PO, CISO en FG adviseren de teamleider en medewerker maatregelen te treffen.

- Do: teamleider en of de medewerker - ofwel eerste lijn - voeren de maatregelen uit.

- Check: PO checkt de privacymaatregelen en CISO checkt de informatiebeveiligingsmaatregelen. FG houdt steekproefsgewijs toezicht op maatregelen en meldt resultaten aan MT en Teamleider.

- Act: Als vervolg op bevindingen van de check wordt het proces zo nodig aangescherpt.



9

[9] PDCA-cyclus voor informatiebeveiliging en privacy - Inergy

Bijlage 1: Rapport M&I voorjaar 2022, samenvatting

In 2022 heeft een extern bureau de privacyvolwassenheid van de gemeente Westerveld doorgelicht.

De belangrijkste bevindingen:

1 Er is een papieren werkelijkheid en een realiteit.

Beleidsstukken en procedures wel zijn beschreven maar zijn in de praktijk niet bekend zijn bij medewerkers. Bewustwording onder management en medewerkers is beperkt. Een deel van de stukken is verouderd en zal na herziening opnieuw moeten worden vastgesteld.

2 Er is geen verwerkingsregister.

Hierdoor is er geen goed overzicht van alle processen binnen Westerveld, kan er geen risicoregister worden opgesteld en is het onbekend wie eigenaren van processen, risico's en maatregelen zijn. Grip op de processen en risico's van Westerveld kan niet worden aangetoond.

3 Het leveranciersmanagement is niet op orde.

Het is niet duidelijk hoe de taken tussen Westerveld en haar leveranciers (met name ONS) verdeeld zijn en er vindt geen controle plaats op leveranciers, hierdoor worden zij niet aan hun afspraken gehouden. Informatiebeveiliging en privacy worden niet altijd vooraf meegenomen bij de inkoop van nieuwe systemen.

4 Westerveld heeft een klein team met hoge doorloop.

Dit geldt zowel voor de formatie van de privacyorganisatie als voor de gehele organisatie. Kennis is niet altijd geborgd doordat er een hoge doorloop is, en role-based access is lastig te creëren doordat personen meerdere rollen hebben. Formatie op de privacy officer is te krap om de achterstanden in te halen

De adviezen:

1.Vernieuw en verkort de documentatie

Update de beleidsstukken, en zorg dat medewerkers in één oogopslag beleidsstukken en procedures kunnen begrijpen. Het AT stelt de nieuwe stukken vast. Start daarnaast met bewustwordingsacties, met name bij leidinggevenden en in het primair proces.

2. Stel registers op.

Stel een verwerkingsregister op, inclusief eigenaren van processen. Gebruik dit als basis voor een risicoregister en BIVclassificaties, en de start met risicomanagement. Hierdoor worden de eerste stappen gezet om sterker procesgericht te werken in de organisatie.

3. Zorg dat leveranciersmanagement wordt opgezet.

Zorg dat informatiebeveiliging en privacy vooraf in het (inkoop)proces meegenomen worden. Maak duidelijke afspraken over informatiebeveiliging en privacy met leveranciers over taken en verantwoordelijkheden, en zorg dat deze gecontroleerd worden door verantwoordelijken binnen Westerveld.

4. Westerveld heeft een klein team (+- 180 werknemers) met hoge doorloop.

Zorg dat het Privacymanagement ysteem (PMS) en Informatiebeveiligingsmanagment-systeem (ISMS) goed bijgehouden worden, om de kennis te borgen, ondanks de hoge doorloop. Qua bezetting van het privacyteam raadt M&I voor FG 0,2 (extern) tot 0,5 fte aan en voor de Privacy Officer (PO) 0,8 tot 1 fte. Voorjaar 2022 is een nieuwe privacy officer gestart voor 0,7 fte, daarvoor was het 0,5 fte. Dit is niet voldoende om de adviezen over documentatie,, register van verwerkingen, leveranciersmanagement uit te kunnen voeren.

Bijlage 2: Uitgevoerde activiteiten cf. Jaarplan Privacy en Informatieveiligheid 2021-2022

1. Bewustwording en organisatorische inbedding

- Meer betrekken organisatie : Nulmeting M&I

- Afstemming binnen nieuwe team Bedrijfsvoering / Staf

  - Communicatieplan en workshops; onboarding medewerkers en Leerveld

  - Crisisplan en bedrijfscontinuïteitsplan

2 Autorisatiemanagement

- Inzicht in autorisaties en meest risicovolle applicaties, overleg over instellen en beheer autorisatiebeheer

- SUWI

3. Risicomanagement en DPIA's

- DPIA's vroegsignalering schulden, Wet Inburgering en dashboard jeugdzorg

- Nieuw Zaaksysteem

4 Verplichte informatie, documenten en processen AVG

- Datalekken afhandelen

- Inzageverzoeken afhandelen

- Register van Verwerkingen

- Standaard verwerkersovereenkomst

5. Anticiperen op ontwikkelingen, w.o. nieuwe wetgeving

- Wet Open Overheid en Wet aanpak meervoudige problematiek in het sociaal domein (gegevensdeling in het sociaal domein) WAMS

  - Fraudeopsporing sociaal domein, online monitoring

  - Vitale Vakantieparken, samenwerking Naober en Drentse gemeenten

  - Samenwerkingsovereenkomsten bij Sociaal Domein (Leerplicht)

  - Nieuwe Zaaksysteem

  - Samenwerkingsovereenkomst leerplicht ZW-Drentse gemeenten

  - Verordening Toeristenbelasting (burgemeester en horeca)

  - Nieuwe Privacy Officer

  - Personeelvolgsysteem beheerder ONS

Bijlage 3: Dreigingsbeeld 2023-2024 van de Informatiebeveligingsdienst van de VNG

De drie belangrijkste dreigingen voor de lokale informatievoorziening die door de Informatiebeveiligingsdienst (IBD) in het tweejaarlijkse 'Dreigingsbeeld informatiebeveiliging gemeenten' worden gesignaleerd zijn:

- Meer ransomware-aanvallen met destructievere gevolgen;
    - Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken.
- Steeds meer en ernstiger kwetsbaarheden in software;
    - Alle hard- en software bevat kwetsbaarheden en fouten. Deze zouden kunnen worden misbruikt door kwaadwillenden. Het is daarom zaak om kwetsbaarheden tijdig te verhelpen
- Weinig zicht op gevaren bij samenwerkingsverbanden en leveranciers.
    - Gemeenten vertrouwen erop dat bij een samenwerkingsverband informatiebeveiliging en privacy 'gewoon geregeld zijn'. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed. Gemeenten zijn in de afgelopen twee jaar regelmatig geconfronteerd met incidenten die ontstaan zijn bij derden waarbij de gevolgen in de eigen gemeente merkbaar waren.